SMALLEST POSETS WITH GIVEN CYCLIC AUTOMORPHISM GROUP

JONATHAN ARIEL BARMAK AND AGUSTÍN NICOLÁS BARRETO

Abstract. For each $n \geq 1$ we determine the minimum number of points in a poset with cyclic automorphism group of order n.

1. Introduction

In 1938 R. Frucht [7] proved that any finite group can be realized as the automorphism group of a graph. Moreover, the graph can be taken with $3d|G|$ vertices, where d is the cardinality of any generator set of G ([8, Theorems 3.2, 4.2]). In 1959 G. Sabidussi [11] showed that in fact $O(|G|\log(d))$ vertices suffice. In 1974 L. Babai proved that the number of generators is not relevant, and with exception of the cyclic groups $\mathbb{Z}_3, \mathbb{Z}_4$ and $\mathbb{Z}_5$, the graph can be taken with just $2|G|$ vertices. Sabbidussi claims in [11] that he was able to compute the smallest number of vertices $\alpha(G)$ in a graph with automorphism group G in the case that G is cyclic of prime power order. Also, he asserts that for $n = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$, $\alpha(\mathbb{Z}_n) = \sum\limits_{i=1}^{k} \alpha(\mathbb{Z}_{p_i^{r_i}})$. Unfortunately both his computations for $\mathbb{Z}_{p^r}$ and the assertion are wrong. In [10] R.L. Meriwether rectifies these errors and correctly determines $\alpha(\mathbb{Z}_n)$ for any $n \geq 1$. However, he commits similar mistakes when trying to extend this computation to arbitrary finite abelian groups. In [1, 2] W. Arlinghaus provides a complete calculation of $\alpha(G)$ for G finite abelian. The proof follows these steps. First compute $\alpha(G)$ for G cyclic of prime power order, then for arbitrary finite cyclic groups, then for abelian p-groups and finally, the general case.

In parallel, the analogous problem was studied for partially ordered sets. In 1946 G. Birkhoff [6] proved that for any finite group G there is a poset of $|G|(|G|+1)$ points and automorphism group isomorphic to G. Then Frucht [9] improved this to $(d+2)|G|$ points. In 1980 Babai [4] proved that $3|G|$ points are enough. However, the smallest number $\beta(G)$ of points of a poset with an arbitrary finite abelian group G of automorphisms has not yet been determined. In this paper we compute $\beta(G)$ for every finite cyclic group G.

Corollary 12. *Let $n = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$, where the p_i are different primes and $r_i \geq 1$ for every i. Then the minimum number $\beta(\mathbb{Z}_n)$ of points in a poset with cyclic automorphism group of order n is $\sum\limits_{i=1}^{k} b(p_i^{r_i})p_i^{r_i} - 1$ if $3|n, 4|n, 9\nmid n$ and $8\nmid n$, and it is $\sum\limits_{i=1}^{k} b(p_i^{r_i})p_i^{r_i}$ otherwise. Here $b(2) = 1$, $b(3) = b(4) = b(5) = b(7) = 3$, and $b(p^r) = 2$ for any other prime power.*

2020 *Mathematics Subject Classification.* 06A11, 20B25, 06A07, 05E18.

Key words and phrases. Posets, Automorphism group.

Both authors were supported by CONICET and partially supported by grant UBACyT 20020190100099BA. The first named author was also partially supported by grants CONICET PIP 11220170100357CO, ANPCyT PICT-2017-2806 and ANPCyT PICT-2019-02338.

This result was first announced in [5]. In [5] we computed first $\beta(G)$ for G cyclic of prime power order, then for arbitrary finite cyclic and for finite abelian p-groups with $p \geq 11$, following the steps of the proof of the graph case exposed by Arlinghaus. The calculation of $\beta(\mathbb{Z}_n)$ in this paper is more direct than the original we gave in [5]. Just as in graphs, the bound $\beta(\mathbb{Z}_n) \leq \sum_{i=1}^{k} \beta(\mathbb{Z}_{p_i^{r_i}})$ holds for $n = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$, but not the equality, in general. For instance $\beta(\mathbb{Z}_{12}) = \beta(\mathbb{Z}_3) + \beta(\mathbb{Z}_4) - 1$. The case of p-groups will not be addressed in this article.

In Section 2 we construct explicit examples which provide an upper bound for $\beta(\mathbb{Z}_n)$. In Section 3 we prove some lemmas concerning the cyclic structure of a generator of $\mathrm{Aut}(P)$ for a poset P with cyclic automorphism group. In the last section we introduce the notion of weight of a prime power in a cycle, which we use in the proof of the lower bound.

2. Construction of the examples

A poset is a set with a partial order $\leq$. The elements of the underlying set of a poset are called points. All posets are assumed to be finite, that is, their underlying set is finite. If P is a poset and $x, y \in P$, we write $x < y$ if $x \leq y$ and $x \neq y$. We say that y covers x if $x < y$ and there is no $x < z < y$. The edges of P are the pairs (x, y) such that y covers x. The Hasse diagram of P is the digraph whose vertices are the points of P and the edges are the edges of P. If the orientation of an arrow is not indicated in the graphical representation of the Hasse diagram, we assume it points upwards. A morphism $P \to Q$ of posets is an order-preserving map, i.e. a function f between the underlying sets such that for every pair $x, y \in P$ with $x \leq y$ we have $f(x) \leq f(y)$. If P is a poset, since it is finite, an automorphism of P is just a permutation of the underlying set which is a morphism. A subposet of a poset P is a subset of the underlying set with the inherited order. Given an automorphism g of a poset P, we say that a subset A of the underlying set of P is invariant or g-invariant if $g(A) = A$. In this case, g induces an automorphism on the subposet with underlying set A.

Definition 1. Define $b(1) = 0$, $b(2) = 1$, $b(3) = b(4) = b(5) = b(7) = 3$. For any other prime power p^r, define $b(p^r) = 2$.

We denote by $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ the additive group of integers modulo n.

Proposition 2. *Let $n = p^r$, where $p \geq 2$ is a prime and $r \geq 0$. Then there exists a poset P with $b(n)n$ points and automorphism group $Aut(P)$ isomorphic to $\mathbb{Z}_n$.*

Proof. For $n = 1$ we take the empty poset and for $n = 2$ we take the discrete poset on 2 points. By discrete we mean an antichain, i.e. a poset of pairwise incomparable elements. If $n = 3, 4, 5, 7$ we use the following well-known general construction [9]: $P = \mathbb{Z}_n \times \{0, 1, 2\}$ with the order $(i, 2) > (i, 1) > (i, 0) < (i+1, 2)$ for every $i \in \mathbb{Z}_n$. It is easy to see that such poset satisfies $\mathrm{Aut}(P) \simeq \mathbb{Z}_n$. Suppose then that $n \geq 8$. We take two copies of $\mathbb{Z}_n$: $A = \mathbb{Z}_n = \{0, 1, \dots, n-1\}$ and $A' = \{0', 1', \dots, (n-1)'\}$. Let $S = \{0, 1, 2, 4\} \subseteq \mathbb{Z}_n$. For $i \in A$ and $j' \in A'$ we set $i < j'$ if $j - i \in S$. Any two elements in the same copy of $\mathbb{Z}_n$ are not comparable (see Figure 1). We will prove that the automorphism group of this poset P is $\mathbb{Z}_n$. It is clear that $G = \mathbb{Z}_n$ acts regularly on each copy of $\mathbb{Z}_n$ by addition, and this gives a faithful action $G \to \mathrm{Aut}(P)$ on P. So G can be seen as a subgroup of $\mathrm{Aut}(P)$. Since each automorphism of P maps $0 \in A$ to another minimal element of P, the order of the $\mathrm{Aut}(P)$-orbit of $0 \in P$ is n. If we prove that the $\mathrm{Aut}(P)$-stabilizer of $0 \in P$ is trivial, then $|\mathrm{Aut}(P)| = n$, so $\mathrm{Aut}(P)$ is isomorphic to G. Let $h \in \mathrm{Aut}(P)$ be such that $h(0) = 0$.

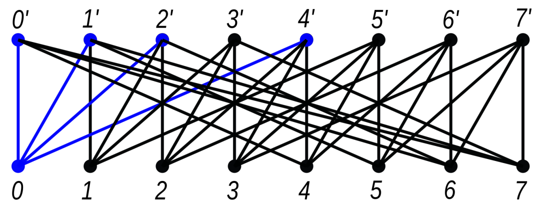

FIGURE 1. The Hasse diagram of P for $n = 8$.

We define the *double neighborhood* $B(i)$ of $i \in A$ as the set of those $j \in A$ such that $\#(P_{>i} \cap P_{>j}) \geq 2$, that is, there are at least two points in A' greater than both, i and j. The *reduced double neighborhood* of $i \in A$ is $\hat{B}(i) = B(i) \smallsetminus \{i\}$. Since h is an automorphism, $B(h(i)) = h(B(i))$ and $\hat{B}(h(i)) = h(\hat{B}(i))$. Given $k \geq 1$, we say that two points $i, j \in A$ are *k-adjacent* if $\#(B(i) \cap B(j)) = k$, and they are *reduced k-adjacent* if $\#(\hat{B}(i) \cap \hat{B}(j)) = k$. Clearly, h preserves k-adjacency and reduced k-adjacency. Suppose first that $n \geq 9$. Then for each $i \in A$, $B(i) = \{i-2, i-1, i, i+1, i+2\}$. It is easy to see that i, j are 4-adjacent if and only if $i - j = \pm 1$. Thus, h induces an automorphism of the cyclic graph on A with edges given by 4-adjacency. Since $h(0) = 0$, h is either the identity $1_{\mathbb{Z}_n}$ or $-1_{\mathbb{Z}_n}$. The second case cannot occur as $\{0, 2, 3, 4\}$ has an upper bound while $\{0, -2, -3, -4\}$ does not. Thus every point of A is fixed by h. If $j' \in A'$, then j' is the unique upper bound of $\{j, j-1, j-2, j-4\}$. Thus $h(j') = j'$. This proves that $h = 1_P$.

Finally, suppose $n = 8$. Given $i \in A$, we have now $\hat{B}(i) = \{i-2, i-1, i+1, i+2, i+4\}$ and $i, j \in A$ are reduced 4-adjacent if and only if $i - j = \pm 3$. Thus, h induces an automorphism in the cyclic graph on A with edges given by reduced 4-adjacency. Then $h = 1_{\mathbb{Z}_n}$ or $-1_{\mathbb{Z}_n}$. The second case cannot occur for the same reason as before. Since each point in A' is determined by the set of smaller points, $h = 1_P$. □

Example 3. There exists a poset P with 20 points and automorphism group isomorphic to $\mathbb{Z}_{12}$.

Take two copies $A = \{0, 1, 2, 3, 4, 5\}$, $A' = \{0', 1', 2', 3', 4', 5'\}$ of $\mathbb{Z}_6$ and two copies $B = \{0'', 1'', 2'', 3''\}$, $B' = \{0''', 1''', 2''', 3'''\}$ of $\mathbb{Z}_4$. The underlying set of P is the union of these four sets. Let $S = \{0, 1, 3\} \subseteq \mathbb{Z}_6$, $T = \{0, 1\} \subseteq \mathbb{Z}_4$. Define the following order in P: $i < j'$ if $j - i \in S$, $i'' < j'''$ if $j - i \in T$, $i''' < j'$ if $j - i$ is even, $i'' < j$ if $j - i$ is even, $i'' < j'$ for every i, j (see Figure 2).

It is clear that $G = \mathbb{Z}_{12}$ acts in each copy of $\mathbb{Z}_6$ and of $\mathbb{Z}_4$ by addition. This induces a faithful action of G on P. If $h \in \mathrm{Aut}(P)$, $h(0'')$ must be a minimal point i'' and $h(0')$ must be a maximal point j'. However i, j cannot have different parity. Indeed, among the points $0, 2, 4, 0''', 1'''$ which cover $0''$, there are just two $0, 0'''$ smaller than $0'$. However, if $i \in \mathbb{Z}_4$ and $j \in \mathbb{Z}_6$ have different parity, among the points covering i'' ($k \in A$ with $k \equiv i(2)$ and $i''', (i+1)'''$) there are three smaller than j': both $j-1, j-3$, and one of $i''', (i+1)'''$. Thus $i \equiv j(2)$, which implies that the $\mathrm{Aut}(P)$-orbit of the set $\{0', 0''\}$ has at most 12 elements. If we prove that the $\mathrm{Aut}(P)$-stabilizer of $\{0', 0''\}$ is trivial, then $|\mathrm{Aut}(P)| \leq 12 = |G|$, so $\mathrm{Aut}(P)$ is isomorphic to G. Let h be an automorphism of P which fixes $0'$ and $0''$.

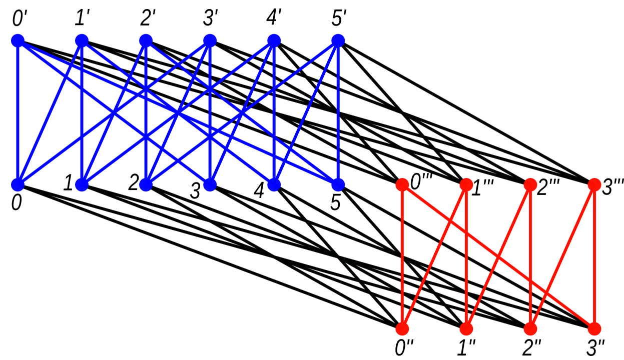

FIGURE 2. A poset P of 20 points and $\mathrm{Aut}(P) \simeq \mathbb{Z}_{12}$.

Note that $2''$ is the unique minimal point different from $0''$ which is covered by three points that cover $0''$. Thus $h(2'') = 2''$. Now, the points of B' are the unique points of P which cover exactly one of $0'', 2''$. Thus B' is invariant. This implies that h restricts to an automorphism of the subposet R with underlying set $B \cup B'$ and of the subposet Q with set $A \cup A'$. Since R is a cycle, there are only two automorphisms of R fixing $0''$. One is the identity and the other maps $0'''$ to $1'''$. However, $0''' < 0'$ while $1''' \not< 0'$. Thus $0'''$ is fixed by h and then h is the identity of R.

Suppose that $i' \in A'$ is a fixed point. Among the points $i, i-1, i-3$ in A covered by i', only $i-1$ and $i-3$ share a lower bound. Thus $h(i) = i$. Similarly, among the points $(i-4)', (i-2)', (i-1)'$ of A' not covering i, only $(i-4)'$ and $(i-2)'$ share a lower bound in B'. Thus $(i-1)'$ is fixed. In conclusion, we showed that i' fixed implies that both i and $(i-1)'$ are fixed. Since $0'$ is fixed, this implies that every point of A and of A' is fixed. Thus $h = 1_P$.

We say that a prime power p^r $(r \geq 1)$ exactly divides an integer n, and write $p^r \parallel n$, if $p^r | n$ and $p^{r+1} \nmid n$.

Theorem 4. *Let $n = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$ where the p_i are different primes and $r_i \geq 1$ for every i. Then there exists a poset with automorphism group isomorphic to $\mathbb{Z}_n$ and $\sum_{i=1}^{k} b(p_i^{r_i})p_i^{r_i} - 1$ points if $3 \parallel n$ and $4 \parallel n$, and with $\sum_{i=1}^{k} b(p_i^{r_i})p_i^{r_i}$ points otherwise.*

Proof. By Proposition 2, for each $1 \leq i \leq k$ there exists a poset P_i with $b(p_i^{r_i})p_i^{r_i}$ points and $\mathrm{Aut}(P_i) \simeq \mathbb{Z}_{p_i^{r_i}}$. The non-Hausdorff join or ordinal sum $P = P_1 \oplus P_2 \oplus \ldots \oplus P_k$ is constructed by taking a copy of each poset and keeping the given ordering in each copy, while setting $x < y$ for each $x \in P_i$ and $y \in P_j$ if $i < j$. Since each automorphism of P preserves heights (the maximum length of a chain with a given maximum element), it restricts to automorphisms of each P_i. Thus $\mathrm{Aut}(P) = \mathrm{Aut}(P_1) \oplus \mathrm{Aut}(P_2) \oplus \ldots \oplus \mathrm{Aut}(P_k) = \mathbb{Z}_n$. If $p_i^{r_i} = 3$ and $p_j^{r_j} = 4$, instead of P_i and P_j we take the poset in Example 3 of $20 = b(3)3 + b(4)4 - 1$ points and automorphism group $\mathbb{Z}_{12}$. $\square$

3. Lemmas

Let X be a finite set, $n \geq 1$ and $x_0, x_1, \ldots, x_{n-1}$ pairwise different elements of X. The cycle $\alpha = (x_0, x_1, \ldots, x_{n-1})$ is the permutation which maps x_i to x_{i+1} (indices considered modulo n) and fixes every other point of X. The number n is the order or length of the cycle, which we denote by $|\alpha|$. A cycle of order n is also called an n-cycle. A cycle α is non-trivial if $|\alpha| \geq 2$. The representation $(x_0, x_1, \ldots, x_{n-1})$ of a non-trivial n-cycle is unique up to cyclic permutation of the n-tuple $x_0, x_1, \ldots, x_{n-1}$. The underlying set of a non-trivial cycle $(x_0, x_1, \ldots, x_{n-1})$ is $\{x_0, x_1, \ldots, x_{n-1}\}$. Many times we will identify a non-trivial cycle with its underlying set. Two non-trivial cycles are disjoint if their underlying sets are. Any permutation g of X can be written as a composition $\alpha_1\alpha_2 \ldots \alpha_k$ of disjoint non-trivial cycles. This representation is unique up to reordering of the cycles. If a cycle α appears in the factorization of g, we say that α is contained in g and write $\alpha \in g$. The orbits of g, or of the action of the cyclic group $\langle g \rangle$ on X, are the underlying sets of the cycles in g and the singletons consisting of fixed points. Disjoint non-trivial cycles commute. Thus, if g is a composition $\alpha_1\alpha_2 \ldots \alpha_k$ of disjoint non-trivial cycles and $m \in \mathbb{Z}$, then $g^m = \alpha_1^m \alpha_2^m \ldots \alpha_k^m$. If α is a cycle of length n and $m \in \mathbb{Z}$, the permutation α^m is a composition of (n, m) =gcd$\{n, m\}$ cycles of length $\frac{n}{(n,m)}$. In particular, α^m is a cycle with the same underlying set as α if n and m are coprime. Moreover, the order of g is the least common multiple of the lengths of its cycles and if a cycle of g has order n, and $m \in \mathbb{Z}$, then g^m fixes every point of the cycle if $n|m$, and fixes no point of the cycle otherwise.

If g is an automorphism of a poset P, then each orbit of g is discrete, as $a < b$ would imply that $a < g^k(a)$ for some $k \in \mathbb{Z}$ and then $\{g^{nk}(a)\}_{n \geq 0}$ would be an infinite chain. If A and B are two different orbits of g we cannot have an element $a \in A$ smaller than another $b \in B$ and at the same time an element $b' \in B$ smaller than another $a' \in A$, as this would imply that $a < b = g^k(b') < g^k(a')$ for some $k \in \mathbb{Z}$, contradicting the fact that A is discrete, or the antisymmetry of the order.

Remark 5. Let P be a poset and let g be an automorphism of P. Let Q be the subposet of points which are not fixed by g. Let $A_0, A_1, \ldots, A_k$ be the orbits of the automorphism induced by g on Q. If h is an automorphism of Q such that $h(A_i) = A_i$ for every i, then it extends to an automorphism of P which fixes every element not in Q.

Indeed, if $x \in P \smallsetminus Q$, $y \in A_i$ and $x < y$, then $h(y) \in A_i$, so there exists $r \geq 0$ such that $g^r(y) = h(y)$. Then $x = g^r(x) < g^r(y) = h(y)$. Similarly, if $x > y$, then $x > h(y)$.

Lemma 6. *Let $n \geq 1$ and let $p^r \neq 2$ be a prime power which exactly divides n. Let P be a poset with Aut(P) cyclic of order n, and let g be a generator of Aut(P). Then g contains at least two cycles of length divisible by p^r.*

Proof. Since g has order n, it contains at least one cycle α of length divisible by p^r. Assume there is no other cycle of length divisible by p^r. The automorphism $g^{\frac{n}{p}}$ fixes then every point not in α. Let x be an element of α and let τ be the transposition of the underlying set of α which permutes x and $g^{\frac{n}{p}}(x) \neq x$. By Remark 5, τ extends to an automorphism h of P which is a transposition. But any power of g either fixes each point in α or fixes no point of α. Since the order of α is at least $p^r > 2$, $h \notin \langle g \rangle = \mathrm{Aut}(P)$, a contradiction. □

If a group G acts on a poset P, an automorphism of P is said to be induced by the action if it is in the image of the homomorphism $G \to \mathrm{Aut}(P)$.

Lemma 7. *Let $p = 3, 5$ or 7. Let P be a poset on which $\mathbb{Z}_p$ acts with exactly two orbits, both of order p. Then there exists an automorphism of P not induced by the action for which each orbit of the action is invariant.*

Proof. Let $g = \alpha\beta \in \mathrm{Aut}(P)$ be the automorphism induced by a generator of $\mathbb{Z}_p$, where $\alpha = (0, 1, \ldots, p-1)$ and $\beta = (0', 1', \ldots, (p-1)')$. If no element of α is comparable with an element of β, then the transposition $(0, 1)$ is an automorphism which is different to g^k for any $k \in \mathbb{Z}$, that is, not induced by the action.

Without loss of generality we can assume then that 0 and $0'$ are comparable, and moreover, that $0 < 0'$. Then no element in β can be smaller than another in α. Since g is an automorphism, $i < i'$ for every $0 \leq i \leq p-1$. If no other pair of elements are comparable, then $(0, 1)(0', 1')$ is an automorphism not induced by the action (it has order 2, for example). If $i < j'$ for every $0 \leq i, j \leq p-1$, then $(0, 1)$ satisfies the desired property. This completes the proof of the case $p = 3$ by the following argument. The case we did not analyze is when P has exactly 6 edges. In that case, let P^c be the *complement* of P, defined as the poset P^c with the same underlying set and setting $i < j'$ if and only if $i \not< j'$ in P, while i, j are not comparable and i', j' are not comparable for every $i \neq j$. Since P and P^c are non-discrete, they have the same automorphisms. As P^c has only 3 edges, there is an automorphism of P^c not induced by the action, so this is the required automorphism of P.

For $p = 5$ we need to consider the case that P has 10 edges. By the complement argument, this will complete the $p = 5$ case. So, suppose $0 < k'$ for some $1 \leq k \leq 4$ (and then $i < (i + k)'$ for every i, where $i + k$ is considered modulo 5). Note that g^k is induced by another generator of $\mathbb{Z}_p$ and it maps i' to $(i + k)'$. Thus, for each $0 \leq i \leq 4$, $i < i'$ and $i < g^k(i')$. Therefore we can assume that $k = 1$. We have then the "symmetry about the axis $03'$", which maps i to $-i$ and j' to $(1 - j)'$ (see Figure 3). This is an automorphism of P which is different to any power of g (it has order 2).

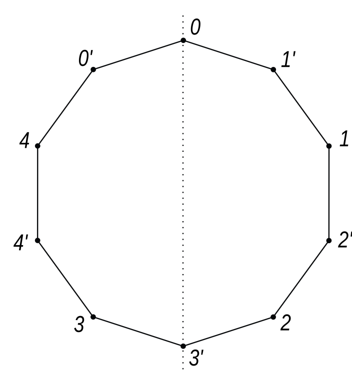

FIGURE 3. The underlying undirected graph of a poset with 10 points and edges $i' > i < (i + 1)'$, and the axis $03'$.

For $p = 7$, if P has 14 edges, then by the argument above we can assume $i' > i < (i+1)'$ for every $0 \leq i \leq 6$ and there is then a symmetry about $04'$. By the complement argument it only remains to analyze the case that P has exactly 21 edges. Here $i < i', (i+k)', (i+l)'$ for certain $1 \leq k \neq l \leq 6$ and again we can assume $k = 1$ by replacing g by g^k. Finally, by replacing g by g^{-1}, it suffices to consider the cases $l = 2, 3$ and 4 (Figure 4).

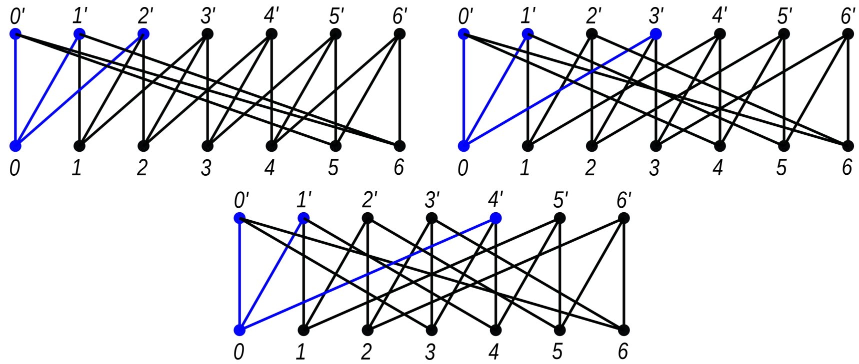

FIGURE 4. Posets with two $\mathbb{Z}_7$-regular orbits and $S = \{0, 1, l\}$ for $l = 2, 3, 4$.

For $l = 2$ we have the involution that maps i to $-i$ and j' to $(2-j)'$. For $l = 3$ we have the following automorphism of order 3: $(142)(356)(0'3'1')(2'4'5')$ (see Figure 5). For $l = 4$, there is again the symmetry about $04'$. □

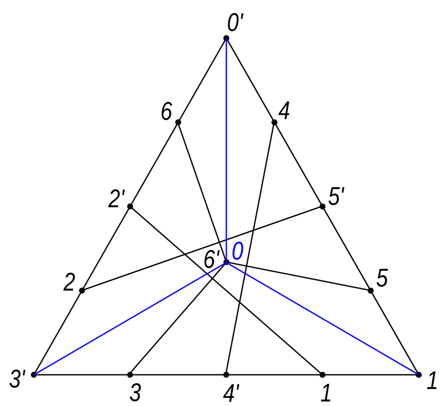

FIGURE 5. The underlying graph of the poset P of 14 points and edges $i < i', (i+1)', (i+3)'$. An automorphism of order 3 is given by a rotation of angle $\frac{2\pi}{3}$.

Lemma 8. *Let P be a poset on which $\mathbb{Z}_4$ acts with exactly two orbits of order 4 or exactly three orbits: two of order 4 and one of order 2. Then there exists an automorphism of P not induced by the action for which each orbit of the action is invariant.*

Proof. Let g be an automorphism induced by a generator of the action and suppose first that $g = (0, 1, 2, 3)(0', 1', 2', 3')$. If P is discrete, $(0, 1)$ satisfies the required conditions. If P has exactly 4 edges, then as in the proof of Lemma 7 we can assume $i < i'$ for every $0 \leq i \leq 3$, and $(0, 1)(0', 1')$ works. By the complement argument we can assume P has exactly 8 edges and that it is determined by the relations $i' > i < (i+k)'$ for some $1 \leq k \leq 3$. The case $k = 3$ reduces to the case $k = 1$ by replacing g by g^3. If $k = 1$, the symmetry $(1, 3)(0', 1')(2', 3')$ about 02 satisfies the required conditions. If $k = 2$, then $(0, 2)$ works.

Suppose then that $g = \alpha\beta\gamma$ with $\alpha = (0, 1, 2, 3)$, $\beta = (0', 1', 2', 3')$, $\gamma = (0'', 1'')$. Let Q be the subposet of points in α and β. Since $g^2 = (0, 2)(1, 3)(0', 2')(1', 3')$, every automorphism of the poset Q which has $\{0, 2\}, \{1, 3\}, \{0', 2'\}, \{1', 3'\}$ as invariant sets, extends to P by Remark 5. If Q is discrete or if Q has 16 edges, then $(0, 2)$ is an automorphism of Q which extends to P and this extension is not induced by the action. If Q has exactly 4 edges, we may assume $i < i'$ for every i and then $(0, 2)(0', 2')$ extends to an automorphism of P different to any power of g. If Q has exactly 12 edges, the complement argument can be used. Suppose then Q has exactly 8 edges. By relabelling we can assume the relations are (a) $i < j'$ for $i \equiv j(2)$ or (b) $i' > i < (i + 1)'$ for every i. In case (a), $(0, 2)$ is again an automorphism which has every nontrivial orbit of g^2 as an invariant set. In the rest of the proof we assume we are in case (b).

If the points of γ are not comparable with any point of Q, then the symmetry about 02 which maps i to $-i$ and j' to $(1 - j)'$, is an automorphism of Q which extends to P, and this extension satisfies the required conditions.

By considering the opposite order, we can assume a point of γ is comparable with a point of α. Moreover, by relabelling if needed we can assume $0''$ is comparable with 0. Suppose first that $0'' < 0$. Since g is an automorphism, then $0'' < 2$ and $1'' < 1, 3$. If $0'' \not< 1$, then $0'' \not< 3$ and $1'' \not< 0, 2$. If $0'' < 1$, then $0'' < 3$ and $1'' < 0, 2$. In either case, the symmetry of Q about 02 extends by the identity to an automorphim of P which is not induced by the action, even though this automorphism of Q does not have the orbits of g^2 as invariant sets. Finally suppose $0'' > 0$. Then $0'' > 2$ and $1'' > 1, 3$. We can assume no element in β is smaller than an element in γ, by the previous case and the duality argument. Also, we cannot have an element of γ being smaller than another j' of β, since this would imply that $i < j' > i + 2$, modulo 4, for certain $0 \leq i \leq 3$, which is absurd. In any case, if $0'' \not> 1$ or if $0'' > 1$, we have that the symmetry of Q about 02 extends to an automorphism of P. □

Lemma 9. *Let $p = 3, 5$ or 7. Let P be a poset with cyclic automorphism group of order $n \geq 1$, and let $g \in Aut(P)$ be a generator. Suppose g contains a p-cycle α and a pk-cycle $\beta \neq \alpha$ for some $p \nmid k \geq 1$. Then it contains a third cycle whose length is divisible by p.*

Proof. Suppose $\beta = (0, 1, \ldots, pk - 1)$. Let Q be the subposet of P whose points are those of α and β. Assume that there is no other cycle in g whose length is divisible by p. In particular $p \parallel n$. Since the order of any cycle of g different from α and β divides $\frac{n}{p}$, the automorphism $g^{\frac{n}{p}}$ fixes every point not in Q. Moreover $g^{\frac{n}{p}}$ has $k + 1$ orbits of order p, which are the underlying set of α and $A_i = \{0 \leq j \leq pk - 1 | \ j \equiv i(k)\}$ for $0 \leq i \leq k - 1$. In particular, by Remark 5 every automorphism of Q for which these sets are invariant extends to an automorphism of P.

Let Q' be the subposet of Q whose points are those of α and A_0. Since g^k induces an automorphism of Q' with two orbits of order p, by Lemma 7 there is an automorphism h of Q' not induced by a power of g^k for which the underlying set of α and A_0 are invariant. We extend h to an automorphism $\overline{h}$ of Q as follows. Let j be a point of β, $0 \leq j \leq kp - 1$. Let $0 \leq i \leq k - 1$ be such that $j \in A_i$. Since $p \nmid k$, there exists a unique $0 \leq t \leq k - 1$ such that $k | j + tp$, in other words $j + tp$, considered modulo kp, lies in A_0. Then $h(j + tp) \in A_0$. Define $\overline{h}(j) = h(j + tp) - tp \in A_i$. We claim that $\overline{h}$ is an automorphism of Q. It is clearly bijective. Two different points of β cannot be comparable as they are in the same orbit. Suppose j in β and a in α are comparable, say $a < j$. Let $0 \leq t \leq k - 1$ be such that $k | j + tp$. Then $a = g^{tp}(a) < g^{tp}(j) = j + tp$. Since h is a morphism, $h(a) < h(j + tp)$. Thus

$\overline{h}(a) = h(a) = g^{-tp}(h(a)) < g^{-tp}(h(j+tp)) = h(j+tp) - tp = \overline{h}(j)$. Since the underlying set of α and each A_i are $\overline{h}$-invariant, $\overline{h}$ extends to an automorphism of P, which must be a power g^r of g. Since g^r leaves A_0 invariant, in particular $r = g^r(0) \in A_0$, so $k|r$ and h is then induced by a power of g^k, a contradiction. □

Lemma 10. *Let P be a poset with cyclic automorphism group of order $n \geq 1$, and let $g \in Aut(P)$ be a generator. Suppose that g contains two 4-cycles α, β. Then it contains a third cycle of length divisible by 4 or two more cycles of even length.*

Proof. The proof is very similar to that of Lemma 9, so we omit details. If α and β are the unique two cycles of even length in g, then by Lemma 8 there is an automorphism h of the poset of points of these two cycles which is not induced by a power of g, and moreover has the underlying sets of α and β as invariant sets. Since the non-trivial orbits of $g^{\frac{n}{4}} \in \mathrm{Aut}(P)$ are the underlying sets of α and β, h extends to an automorphism of P, a contradiction.

Suppose then there exists a third cycle $\gamma = (1, 2, \ldots, 2k)$ in g with k odd, and that there is no other cycle of even length. We define Q to be the subposet whose points are those of α, β and γ. Then $g^{\frac{n}{4}}$ fixes every point not in Q. The other orbits of $g^{\frac{n}{4}}$ are the underlying sets of α and β, and $A_i = \{i, k+i\}$ for $0 \leq i \leq k-1$. Let Q' be the subposet whose points are those of α, β and A_0. Then g^k induces an automorphism of Q' and by Lemma 8 there is an automorphism h of Q' which is not induced by a power of g^k, and for which the underlying sets of α, β and A_0 are invariant. We extend it to an automorphism $\overline{h}$ of Q by defining $\overline{h}(j) = h(j+4t) - 4t$, where t is such that $k|j+4t$. Then $\overline{h}$ is bijective, it is a morphism and leaves each A_i invariant. It extends to an automorphism of P, say g^r. Since g^r leaves A_0 invariant, then $k|r$, which implies that h is induced by a power of g^k, a contradiction. □

4. Weights and the lower bound

Let g be a permutation of order n of a finite set X. Let α be a cycle in g of length $l = p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}$, where the p_i are distinct prime integers, $r_i \geq 1$ for every i. For each prime power p^r we will define a weight $w_{p^r}(\alpha) \in \mathbb{R}_{\geq 0}$ which depends on p^r, l and n, in such a way that $\sum_{p^r} w_{p^r}(\alpha) p^r = l$, where the sum is taken over all prime powers dividing n. In particular $\#X \geq \sum_{p^r \| n} (\sum_{\alpha \in g} w_{p^r}(\alpha)) p^r$. For each $l \geq 2$ we will assign the weight of every prime power p^r in a cycle α of length $|\alpha| = l$ according to a series of rules. In every case, if the weight $w_{p^r}(\alpha)$ is not explicitly defined for some prime power, we assume it is 0.

Exception 6. Suppose $l = 6$. If $3 \parallel n$ then $w_3(\alpha) = 2$. If $3 \nparallel n$ and $2 \parallel n$, then $w_2(\alpha) = 3$. If $3 \nparallel n$ and $2 \nparallel n$, then $w_4(\alpha) = \frac{3}{2}$.

Exception 12. Suppose $l = 12$. If $3 \parallel n$ then $w_3(\alpha) = 4$. If $3 \nparallel n$, then $w_4(\alpha) = 3$.

Exception 10-14. Suppose $l = 2p$ for $p = 5$ or 7. If $2 \parallel n$, $w_2(\alpha) = 1$. Otherwise $w_4(\alpha) = \frac{1}{2}$. In any case $w_p(\alpha) = \frac{2(p-1)}{p}$.

General case. Suppose $l = p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k} \neq 6, 12, 10, 14$, where the p_i are different primes and each $r_i \geq 1$. For each $1 \leq i \leq k$, we define $w_{p_i^{r_i}}(\alpha) = \frac{\prod_{j \neq i} p_j^{r_j}}{k}$, unless $p_i^{r_i} = 2$ and $2 \nparallel n$.

In that case, $w_2(\alpha) = 0$, while $w_4(\alpha) = \frac{\prod_{j\neq i} p_j^{r_j}}{2k}$. In particular, if $l = p^r \geq 3$ is a prime power, $w_{p^r}(\alpha) = 1$.

Note that, as we required, the sum $\sum_{p^r|n} w_{p^r}(\alpha)$ over all the prime powers dividing n is the length l of α. Note also that if $l = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$, then $w_{p^r}(\alpha) \neq 0$ only if $p^r = p_i^{r_i}$ for some $1 \leq i \leq k$ or $p^r = 4$.

Theorem 11. *Let $n \geq 1$. Let P be a poset with $Aut(P)$ cyclic of order n generated by g. Let p^r be a prime power which exactly divides n. If $p^r \neq 2, 4$ then $\sum_{\alpha\in g} w_{p^r}(\alpha) \geq b(p^r)$. If $3 \nmid n$ and $p^r = 2$ or $p^r = 4$, $\sum_{\alpha\in g} w_{p^r}(\alpha) \geq b(p^r)$ as well. If $3 \parallel n$ and $2 \parallel n$, $\sum_{\alpha\in g}(2w_2(\alpha) + 3w_3(\alpha)) \geq 2b(2) + 3b(3) = 11$. Finally, if $3 \parallel n$ and $4 \parallel n$, $\sum_{\alpha\in g}(4w_4(\alpha) + 3w_3(\alpha)) \geq 4b(4) + 3b(3) - 1 = 20$.*

Proof. If $p^r \neq 2, 3, 4, 5, 7$, by Lemma 6, there are at least two cycles of length divisible by p^r. By hypothesis their lengths are not multiples of p^{r+1}. But if α is a cycle of g whose length is a multiple of p^r, then $w_{p^r}(\alpha) \geq 1$. Indeed, the weights in α are assigned according to the General case. If the length of α is $l = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$, we can assume $p^r = p_1^{r_1}$ and then $w_{p^r}(\alpha) = \frac{\prod_{j=2}^{k} p_j^{r_j}}{k} \geq \frac{2^{k-1}}{k} \geq 1$. Thus, $\sum_{\alpha\in g} w_{p^r}(\alpha) \geq 2 = b(p^r)$.

Suppose now $p^r = 5$. If α is a cycle of g of length $l = 5$, then $w_5(\alpha) = 1$. If $l = 10$, then $w_5(\alpha) = \frac{8}{5} \geq \frac{3}{2}$ (Exception 10-14). If $l = 5s$ with $s = p_2^{r_2} p_3^{r_3} \dots p_k^{r_k} \geq 3$ not divisible by 5, then either $k = 2$, or $k \geq 3$. In the first case $w_5(\alpha) = \frac{s}{2} \geq \frac{3}{2}$, and in the second case $w_5(\alpha) = \frac{\prod_{j=2}^{k} p_j^{r_j}}{k} \geq \frac{2^{k-2}.3}{k} \geq 2 \geq \frac{3}{2}$.

By Lemma 6, there are at least two cycles of length divisible by 5 (and not by 5^2). Suppose first there exactly two such cycles, α and α'. None of them can be of length 5 by Lemma 9. Thus $w_5(\alpha) + w_5(\alpha') \geq 2.\frac{3}{2} = 3 = b(5)$. Finally, if there are at least three cycles in g of length divisible by 5, then $\sum_{\alpha\in g} w_5(\alpha) \geq 3 = b(5)$.

The case $p^r = 7$ is similar to the previous one, with the observation that for length $l = 14$, $w_7(\alpha) = \frac{12}{7} \geq \frac{3}{2}$ (Exception 10-14). So, also in this case $\sum_{\alpha\in g} w_7(\alpha) \geq 3 = b(7)$.

Let $p^r = 3$. If the length of a cycle α in g is $l = 3$, $w_3(\alpha) = 1$. If $l = 6$, $w_3(\alpha) = 2$ (Exception 6). If $l = 12$, $w_3(\alpha) = 4$ (Exception 12). If $l = 3s$ with $s = p_2^{r_2} p_3^{r_3} \dots p_k^{r_k} \geq 5$, then either $k = 2$, or $k \geq 3$. In the first case $w_3(\alpha) = \frac{s}{2} \geq \frac{5}{2}$, and in the second case $w_3(\alpha) = \frac{\prod_{j=2}^{k} p_j^{r_j}}{k} \geq \frac{2^{k-2}.3}{k} \geq 2$.

By Lemma 6 there are at least two cycles in g of length divisible by 3 (and not by 3^2). Suppose first there are exactly two such cycles α and α'. None of them can have length 3 by Lemma 9. Then $w_3(\alpha)+w_3(\alpha') \geq 2.2 = 4 \geq 3 = b(3)$. Finally, if there are at least three cycles in g of length divisible by 3, then $\sum_{\alpha\in g} w_3(\alpha) \geq 3 = b(3)$. Note that $\sum_{\alpha\in g} w_3(\alpha) \geq 4$ unless there are exactly three cycles of length 3 and no other cycle of length divisible by 3.

We analyze now the case that $3 \nmid n$ and $p^r = 2$ or 4. In the first situation, there is at least one cycle α of even length l (not divisible by 4). If $l = 2$, $w_2(\alpha) = 1$ (General case). If $l = 6$, $w_2(\alpha) = 3$ (Exception 6). If $l = 10$ or $l = 14$, then $w_2(\alpha) = 1$ (Exception 10-14). If $l = 2s$ with $s = p_2^{r_2} p_3^{r_3} \dots p_k^{r_k} \neq 1, 3, 5, 7$ (odd), then $w_2(\alpha) = \frac{\prod_{j=2}^{k} p_j^{r_j}}{k} \geq \frac{3^{k-1}}{k} \geq \frac{3}{2}$. Thus $\sum_{\alpha \in g} w_2(\alpha) \geq 1 = b(2)$. We consider the second situation, $p^r = 4$. If α has length $l = 4$, then $w_4(\alpha) = 1$. If $l = 12$, $w_4(\alpha) = 3$ (Exception 12). If $l = 4s$ with $s = p_2^{r_2} p_3^{r_3} \dots p_k^{r_k} \geq 5$ (odd), then $k = 2$ or $k \geq 3$. For $k = 2$ we have $w_4(\alpha) = \frac{s}{2} \geq \frac{5}{2}$. For $k \geq 3$, $w_4(\alpha) \geq \frac{3^{k-1}}{k} \geq 3$. By Lemma 6, g contains at least two cycles of lengths divisible by 4 (and not by 8). Suppose first there are exactly two such cycles, α and α', of lengths l, l'. If $l = l' = 4$, then by Lemma 10, there exists a third and a fourth cycle β, β' of lengths $2m$ and $2m'$ for some odd m, m'. The weights $w_4(\beta)$ that we obtain for each m are the halves of the weights that we obtained for 2 in cycles of the same length when $2 \parallel n$. Namely, if $m = 1$, $w_4(\beta) = \frac{1}{2}$ (General case); if $m = 3$, $w_4(\beta) = \frac{3}{2}$ (Exception 6); if $m = 5, 7$, $w_4(\beta) = \frac{1}{2}$ (Exception 10-14); if $m = p_2^{r_2} p_3^{r_3} \dots p_k^{r_k} \neq 1, 3, 5, 7$ then $w_4(\beta) \geq \frac{3^{k-1}}{2k} \geq \frac{3}{4}$ (General case).

The same happens with β'. Thus $w_4(\alpha) + w_4(\alpha') + w_4(\beta) + w_4(\beta') \geq 1 + 1 + \frac{1}{2} + \frac{1}{2} = 3 = b(4)$. If instead $l = 4$ and $l' = 12$, then $w_4(\alpha) + w_4(\alpha') = 1 + 3 = 4 > 3$. If $l = 4$ and $l' = 4s$ for some odd $s \geq 5$, then $w_4(\alpha) + w_4(\alpha') \geq 1 + \frac{5}{2} > 3$. If both l and l' are greater than 4, then $w_4(\alpha) + w_4(\alpha') \geq \frac{5}{2} + \frac{5}{2} > 3$. Finally, if there are at least three cycles of length divisible by 4, then $\sum_{\alpha \in g} w_4(\alpha) \geq 3$. Thus, in any case $\sum_{\alpha \in g} w_4(\alpha) \geq 3 = b(4)$.

It only remains to analyze the case $3 \parallel n$ and $2 \parallel n$ and the case $3 \parallel n$ and $4 \parallel n$. If $3 \parallel n$ and $2 \parallel n$, recall that we have already proved that $\sum_{\alpha \in g} w_3(\alpha) \geq 4$ or there are exactly three cycles of length 3 and no other cycle of length divisible by 3. In the first case $\sum_{\alpha \in g} (2w_2(\alpha) + 3w_3(\alpha)) \geq \sum_{\alpha \in g} 3w_3(\alpha) \geq 12$. In the second case, there exists a cycle β in g of even length $m \neq 6$, so $w_2(\beta) \geq 1$. Thus $\sum_{\alpha \in g} (2w_2(\alpha) + 3w_3(\alpha)) \geq 2.1 + 3.3 = 11$.

The last case is $3 \parallel n$ and $4 \parallel n$. Note that if there are no cycles of length 6 nor 12 in g, then the computation $\sum_{\alpha \in g} w_4(\alpha) \geq 3$ remains valid as Exceptions 6 and 12 do not occur. Thus $\sum_{\alpha \in g} (3w_3(\alpha) + 4w_4(\alpha)) \geq 3.3 + 4.3 = 21 > 20$. If there are at least two 12-cycles, then $\sum_{\alpha \in g} (3w_3(\alpha) + 4w_4(\alpha)) \geq 2.3.4 = 24 > 20$. If there is no 12-cycle in g and $\sum_{\alpha \in g} w_4(\alpha) < 3$, then we must be in the case that there is a 6-cycle. This already implies $\sum_{\alpha \in g} w_3(\alpha) \geq 4$, while the existence of two cycles of length divisible by 4 implies $\sum_{\alpha \in g} w_4(\alpha) \geq 2$. Thus $\sum_{\alpha \in g} (3w_3(\alpha) + 4w_4(\alpha)) \geq 3.4 + 4.2 = 20$.

Thus we may assume g has a unique 12-cycle. By Lemma 6 there is another cycle of length divisible by 4, so $\sum_{\alpha \in g} w_4(\alpha) \geq 1$. On the other hand, $\sum_{\alpha \in g} w_3(\alpha) \geq 4 + 2 = 6$, as the weight of 3 in a 12-cycle is 4 and by Lemmas 6 and 9 there are either two more cycles of lengths divisible by 3 or just one, but of length not 3. Thus $\sum_{\alpha \in g} (3w_3(\alpha) + 4w_4(\alpha)) \geq 3.6 + 4.1 = 22 > 20$. □

Corollary 12. *Let $n = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$, where the p_i are different primes and $r_i \geq 1$ for every i. Then the minimum number $\beta(\mathbb{Z}_n)$ of points in a poset with cyclic automorphism group of order n is $\sum_{i=1}^{k} b(p_i^{r_i}) p_i^{r_i} - 1$ if $3 \parallel n$ and $4 \parallel n$, and $\sum_{i=1}^{k} b(p_i^{r_i}) p_i^{r_i}$ otherwise.*

Proof. If P is a poset with $\mathrm{Aut}(P) \simeq \mathbb{Z}_n$ generated by g, then the number of points in P is at least $\sum_{\alpha \in g} |\alpha| = \sum_{\alpha \in g} \sum_{p^r | n} w_{p^r}(\alpha) p^r \geq \sum_{i=1}^{k} (\sum_{\alpha \in g} w_{p_i^{r_i}}(\alpha)) p_i^{r_i}$. If both 3 and 4 exactly divide n, by Theorem 11 this is $\sum_{p_i^{r_i} \neq 3,4} (\sum_{\alpha \in g} w_{p_i^{r_i}}(\alpha)) p_i^{r_i} + \sum_{\alpha \in g} (3w_3(\alpha) + 4w_4(\alpha)) \geq \sum_{p_i^{r_i} \neq 3,4} b(p_i^{r_i}) p_i^{r_i} + 3b(3) + 4b(4) - 1 = \sum_{i=1}^{k} b(p_i^{r_i}) p_i^{r_i} - 1$. Otherwise, the bound is one more than this number. The bound is attained by Theorem 4. □

References

[1] W.C. Arlinghaus. *The structure of minimal graphs with given abelian automorphism group.* Ph.D. Thesis, Wayne State University, 1979.

[2] W.C. Arlinghaus. *The classification of minimal graphs with given abelian automorphism group.* Mem. Amer. Math. Soc. 57(1985), no. 330, viii+86.

[3] L. Babai. *On the minimum order of graphs with given group.* Canad. Math. Bull. 17(1974), no. 4, 467-470.

[4] L. Babai. *Finite digraphs with given regular automorphism groups.* Period. Math. Hungar. 11(1980), no. 4, 257-270.

[5] A.N. Barreto. *Sobre los posets más chicos con grupo de automorfismos abeliano dado.* Tesis de Licenciatura, Universidad de Buenos Aires, 2021.

[6] G. Birkhoff. *Sobre los grupos de automorfismos.* Rev. Un. Mat. Argentina 11(1946), 155-157.

[7] R. Frucht. *Herstellung von Graphen mit vorgegebener abstrakter Gruppe.* Compositio Math. 6(1939), 239-250.

[8] R. Frucht. *Graphs of degree 3 with given abstract group.* Canad. J. Math. 1(1949) 305-378.

[9] R. Frucht. *On the construction of partially ordered systems with a given group of automorphisms.* Amer. J. Math. 72(1950), 195-199.

[10] R. L. Meriwether. *Smallest graphs with a given cyclic group.* 1963, unpublished.

[11] G. Sabidussi. *On the minimum order of graphs with given automorphism group.* Monatsh. Math. 63(1959), 124-127.

Universidad de Buenos Aires. Facultad de Ciencias Exactas y Naturales. Departamento de Matemática. Buenos Aires, Argentina.

CONICET-Universidad de Buenos Aires. Instituto de Investigaciones Matemáticas Luis A. Santaló (IMAS). Buenos Aires, Argentina.

E-mail address: jbarmak@dm.uba.ar

E-mail address: abarreto@dm.uba.ar